WISCONSIN AIR NATIONAL GUARD
ACTIVE GUARD RESERVE (AGR) VACANCY ANNOUNCEMENT

ANNOUNCEMENT NUMBER: 23-092 ANG

OPENING DATE: 20 April 2023 **APPLICATIONS WILL BE ACCEPTED UNTIL:** 11:59PM ON 5 May 2023

POSITION TITLE: Cyber Defense **AFSC REQUIREMENTS:** 1D751X

SKILL LEVEL REQUIRED: 5

MINIMUM RANK: E4 **MAXIMUM RANK:** E6

UNIT/LOCATION: 128th Air Refueling Wing, Milwaukee, WI

AREA OF CONSIDERATION: Open to anyone eligible to join the WI ANG AGR program

APPOINTMENT FACTORS

1. Initial tours will be 3 years. Follow-on tour lengths may be from 1 to 6 years per ANGI 36-101.
2. Non AGR Person receiving a federal military retirement or retainer pay are not eligible.
3. Must meet the physical requirements of DAFI 36-2905, prior to being placed on AGR tour.
4. Members who are not suitable for Career AGR may be considered for an Occasional Tour.
5. Military grade will not exceed the maximum authorized grade on the unit manning document.
6. Must meet all AGR requirements of ANGI 36-101 and AFSC requirements of AFECD/AFOCD.
7. IAW ANGI 36-101, paragraph 5.10, applicants should be able to complete 20 years of active federal service prior to Mandatory Separation Date (MSD). Individuals selected for AGR tours that cannot attain 20 years of active federal Service prior to reaching mandatory separation must complete a Statement of Understanding contained in Attachment 3 of ANGI36-101 and obtain TAG waiver approval prior to starting AGR tour.
8. IAW ANGI 36-101, paragraph 6.6.1., members should remain in the position to which initially assigned for a minimum of 24 months. TAG may waive this requirement when in the best interest of the unit, State, or Air National Guard.
9. Hiring of an E-8/9 or O4+ is contingent on controlled grade availability.
10. IAW ANGI 36-101, paragraph 5.7, an individual must not have been previously separated for cause from active duty or previous Reserve Component AGR tour.

BRIEF DESCRIPTION OF DUTIES:

Responds to disruptions within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, along with response and recovery approaches to maximize survival of life, preservation of property, and information security. Investigates and analyzes relevant response activities and evaluates the effectiveness of and improvements to existing practices. Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware, software, and documentation that are required to effectively manage network defense resources. Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. Uses data collected from a variety of cyber defense tools (e.g., Intrusion detection system alerts, firewalls, network traffic logs.) to analyze events that occur within their environments for the purposes of mitigating threats. Conducts threat and vulnerability assessments and determines deviations from acceptable configurations or policies. Assesses the level of risk and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. Performs assessments of systems and networks within the Network Environment (NE) or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. Collects, processes, preserves, analyzes, and presents computer-related artifacts in support of network vulnerability mitigation. Performs and supports cyber mission Planning, Briefing, Execution, and Debriefing (PBED). Identifies, validates and synchronizes resources to enable integration during the execution of defensive cyber operations. Oversees the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include Communications Security (COMSEC), Emissions Security (EMSEC), Computer Security (COMPUSEC), personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources. Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives. Installs, configures, troubleshoots, and maintains server and systems configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Administers server-based systems, security devices, distributed applications, network storage, messaging, and performs systems monitoring. Consults on network, application, and customer service issues to support computer systems' security and sustainability. Manages and administers integrated methods, enabling the organization to identify, capture, catalog, classify, retrieve, and share intellectual capital and information content. The methods may include utilizing processes and tools (e.g., databases, documents, policies, procedures) and expertise pertaining to the organization. Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices. Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results. Utilizes on the development process of the system development lifecycle. Makes daily product decisions, works on a collaborative team, pairs with team members, and helps ensure user satisfaction using Lean and Agile methodologies. Works with the project team, leadership, stakeholders, and other PMs to progress the goal of shipping the right product to users. Ensures that the product is successful in terms of user value, stakeholder value, and organizational business goals. Consults with stakeholders to guide, gather, and evaluate functional and security requirements. Translates these requirements into guidance to stakeholders about the applicability of information systems to meet their needs. Develops, administers, and secures databases, data management systems, and/or data processes for the storage, query, and utilization of data. Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes. Locates patterns in large data sets using computer science techniques to help team members with different levels of understanding and expertise to make data driven business decisions that increase effectiveness or efficiency of operational forces. Provides end users tiered-level customer support by coordinating software, hardware, and network configuration, troubleshooting, resolution, security, maintenance, and training. Test, implements, deploys, maintains, sustains, troubleshoots, repairs, and administers standard and filed expedient radio frequency wireless, line-of-sight, beyond line-of-sight, wideband, and ground-based satellite and encryption transmission devices (infrastructure and hardware). Includes multiple waveform systems, establishes and maintains circuits, configures and manages system and network connectivity.

SPECIALTY QUALIFICATIONS:

Knowledge. Knowledge is mandatory of principles, technologies, capabilities, limitations, and cyber threat vectors of servers, clients, operating systems, databases, networks and related hardware and software, cybersecurity principles including; national and international laws, policies, and ethics related to operational cybersecurity; operational risk management processes; and specific operational impacts of lapses in cybersecurity.

Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses in Science, Technology, Engineering, and Mathematics (STEM) are desirable. Associate degree or higher in related fields and/or Information Technology (IT) certification is desirable.

Training. For award of the 1D731X, completion of the suffix-specific course is mandatory.

Other. The following are mandatory as indicated: Prior qualification of attaining and maintaining an Information Assurance Technical Level II or Information Assurance Manager Level I certification IAW DoD 8570.01-M, Information Assurance Workforce Improvement or obtaining of certification within six months of selection. Program for retraining can waive minimum ASVAB requirements. For award and retention of these AFSCs: Must attain and maintain a minimum certification level based in position requirements IAW AFMAN 17-1303, Cybersecurity Workforce Improvement Program and DoD 8570.01-M, Information Assurance Workforce Improvement Program, as specified by AFSC shred: 1D7X1. For 1D7X1D, a minimum based on position requirements. Or a minimum of an Information Assurance Management Level I certification. For 1D7X1X, a minimum based on position requirements. Or a minimum of an Information Assurance Technical Level II certification. Must maintain local network access IAW AFI 17-130, Cybersecurity Program Management and AFMAN 17-1301, Computer Security. Specialty may require routine access to Tier 5 (T5) information, systems or similar classified environments. Completion of a background investigation according to AFMAN 16-1405, Personnel Security Program Management, is mandatory by AFSC shred specified: For 1D7X1, For 1D7X1A, completion of a current Tier 5(T5), Top Secret. For 1D7X1B, completion of a current Tier 5 (T5), Top Secret. For 1D7X1D, completion of a current Tier 5 (T5), Top Secret. For 1D7X1E, completion of a current Tier as specified by position requirements. For 1D7X1K, completion of a current Tier as specified by position requirements. For 1D7X1R, completion of a current Tier as specified by position requirements. For 1D7X1Z, completion of a current Tier 5 (T5), Top Secret. NOTE: Award of the 3-skill level without a completed Tier 5 Investigation is authorized provided an interim Top-Secret clearance has been granted according to AFMAN 16-1405.

APPLICATION REQUIREMENTS:

Interested applicants must submit the following documentation to be considered for interview. Any missing items are encouraged to be documented with an explanation in the cover letter included in the application.

APPLICATIONS WILL INCLUDE (All documents must be personally identifiable and must include date if required)

- □ Cover letter with Job Announcement Number and Position Title for which you are applying, current Military Status (AGR, Technician, Traditional, Active Duty), along with contact information (i.e. Phone numbers and an e-mail address).

- □ **NGB Form 34-1** (Application for AGR Position) dated 20131111 **(must be signed and dated).** Manually signed copy accepted. Digital signature may fall off when combining PDF files. Double check prior to sending packet.

- □ **Record Review RIP** (NOT point credit summary, SURF or Career Data Brief) complete and current. Other Service Components submit appropriate individual personnel information printout. This is used to verify AFSCs, aptitude scores, position status, time in service, time in grade, etc. This can be pulled from vMPF.

- □ **Current Fitness Report**. Current (within 12 months) Fitness report from myFitness in pdf format

- □ **AF Form 422** Current (within 12 months)**,** Physical Profile Serial Report. Other Service Components submit medical documentation that includes PULHES score. If any PULHES are a “3”, a statement indicating that individual is Worldwide Deployable needs to be submitted.

- □ **SF 181-** (Race and Ethnicity Identification). Form is required for packet. However, completion is voluntary. Please see further instructions on the form.

- □ All Other Service Component applicants must have their **ASVAB** raw scores converted to Air Force ASVAB scores and include them in a letter from either a Recruiter or MEPS Counselor.

NOTE:

1. Failure to provide all the required documents will result in being disqualified.
2. Applicants must sign NGB Form 34-1; failure to sign the form will result in being disqualified. Please ensure 34-1 reflects Tour Announcement number and current telephone number.
3. If selected for the job, member must have a current passing fitness and an AGR qualified AF Form 422 Signed by the State Air Surgeon prior to being placed on AGR tour.

APPLICATION PROCEDURES

Interested applicants who meet the eligibility criteria may apply by emailing all required documents, as one (1) pdf to TSgt Lachance at michelle.lachance@us.af.mil or SSgt Donais jennifer.donais@us.af.mil. Portfolio formats are accepted. The file and email subject line should read as: LastName, FirstName_#_JobTitle (i.e. Doe, John_22-001_Personnel) An email will be sent to confirm receipt of application. Feel free to call Comm (608) 242-3761 or (608) 242-3135 to verify receipt of your application. Applications will not be reviewed before the closing date.

HOW TO COMBINE/MERGE A PDF:

1. Click Tools
2. Click Combine Files
3. Drag and drop your PDFs into the PDF combiner.
4. Rearrange individual pages or entire files in the desired order.
5. Add more files, rotate or delete files, if needed.
6. Click 'Merge PDF!' to combine and download your PDF

HOW TO CREATE A PORTFOLIO:

1. Click Tools
2. Click Create PDF
3. Click Multiple Files
4. Click Create PDF Portfolio and Next
5. Drag and drop your PDFs into the PDF combiner
6. Rearrange individual pages or entire files in the desired order
7. Click ‘Create!’ to combine and download your PDF